Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of:	)	
	)	
Boulder Regional Emergency Telephone Service Authority Petitions	)	PS Docket 19-254
	)	
	)	
	)	
	)	

COMMENTS OF MUTUALINK, INC.

I. Statement of Interest

Mutualink, Inc., is a Connecticut based corporation that develops and furnishes real time multimedia interoperability solutions to US public safety agencies and critical infrastructure entities ("Mutualink"). Mutualink enables agencies to dynamically and securely interoperate, on demand, by bridging otherwise incompatible and/or disparate voice communications systems, including LMR and push to talk over cellular (PoC), and enabling the secure sharing of other media resources such as video and data resources. Mutualink has over 10,000 active public safety and secondary user endpoints operating across a nationwide virtual network ranging from federal, state and local entities. As such, Mutualink and its public safety customers have a substantial interest in this matter.

II. Interoperability is a Fundamental Requirement of FirstNet

The impetus for FirstNet was driven by a well-known (and today still persistent) public safety agency problem - the inability or in other cases the limited ability of public agencies to effectively communicate and coordinate with one another. This problem came to the forefront of the public consciousness in the aftermath of the September 11th terrorist attack on US soil. The issue was identified in the 9/11 Commission Report[1], and resulted in a specific recommendation:

> *"Congress should support pending legislation which provides for the expedited and increased assignment of radio spectrum for public safety purposes. Furthermore, high-risk urban areas such as New York City and Washington, D.C., should establish signal corps units to ensure communications connectivity between and among civilian authorities, local first responders, and the National*

[1] The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States (9/11 Report), 2004.

Guard. Federal funding of such units should be given high priority by Congress."[2]

47 U.S. Code §1422(a) establishes the First Responder Network Authority ("FNRA") and charges it with "ensur[ing] the establishment of a nationwide, interoperable public safety broadband network." The phrase "nationwide, interoperable public safety broadband network" is given its scope and meaning under §1422(b) by setting forth two primary components a "core network" under paragraph (1) and "radio access network" under paragraph (2). However, this would be an unduly narrow and incorrect interpretation. In fact, the network while being identified as a singular national network is nonetheless more. §1422(b) states that the network is a "national network architecture that evolves with technological advancements and initially consists of (*emphasis added*)" the two components listed in its subparagraphs (1) and (2).

When considered in the context of its intended purpose, the express provisions contemplating evolution and a definitional construct which is clearly identified as being "initial", Congress clearly recognized that the scope of a national network intended for public safety use would necessarily encompass the need to interact with the externalities of a real world environment comprised of other systems, networks and devices in which information and media would be exchanged. In fact, this is already implicitly recognized under §1422(b)1(B) which states that the core network shall "[provide] the connectivity between —

(i) the radio access network; and
(ii) the public Internet or the public switched network, or both.."

Currently, it is well known that public safety agencies utilize a wide variety of communication systems to suit their specific jurisdictions. These include private radio networks which have historically predominated the public safety landscape and have utilized proprietary standards which have effectively isolated these systems into their own silos. Efforts to enable interoperability between radio networks has largely failed through the adoption of industry driven P25 standards due to opportunistic licensing models that make ISSI based interconnection cost prohibitive. The ability to overcome these private siloes is amplified by the highly concentrated market share enjoyed by Motorola within the public safety space. Moreover, this power is leveraged to the detriment of open and fair competition and innovation when access to new products such as push to talk over cellular which tied or made available nearly exclusively to these proprietary radio environments.

If FirstNet is to meet its intended objectives and achieve wide scale adoption it must necessarily provide a means for these external systems (whether they are proprietary radio systems, information systems, IoT systems or the like) to interoperate with FirstNet and enable users to receive, send, transform and exchange information.

[2] Id at p.397.

III. Interoperability with Other Wireless Networks is Expected and Required

47 U.S.C.§ 1426(c)(5) provides that the FRNA among its mandated duties and responsibilities shall:

"…negotiate and enter into, as it determines appropriate, roaming agreements with commercial network providers to allow the nationwide public safety broadband network to roam onto commercial networks and gain prioritization of public safety communications over such networks in times of an emergency."

This is an acknowledgement that the allocated FirstNet spectrum cannot be expected to duplicate the nationwide coverage of all existing commercial networks, and that roaming to other networks is both expected and required.

The legislation further requires that FirstNet be based upon commercial LTE standards; these standards are developed by the 3GPP international standards development organization. Since the legislation was enacted, 3GPP has developed a set of Mission Critical (MCx) protocols to enable enhanced public safety communications over commercial LTE networks. These standards enable LTE networks to carry prioritized real-time Push-to-Talk (MCPTT) voice, video, and data, all of which directly address the communication needs of public safety agencies and hence are being adopted by FirstNet.

The 3GPP MCx standards include an inter-carrier interface (the MCPTT-10 interface) that defines the standard mechanism for MCx communications to flow between carriers. Similar to how voice calls are placed between carriers or how a voice call is placed by a roaming user, the MCPTT-10 interface enables MCPTT calls to be placed between carriers and enables roaming users to place MCPTT calls. Therefore, implementing the MCPTT-10 interface for interoperability with other carriers is required to allow FirstNet users "*to roam onto commercial networks and gain prioritization of public safety communications over such networks*".

We would note, along these lines, that in the implementation of any network to network interoperability there are security and control considerations at an agency domain level that require a means of ensuring agency level access and control between and among its counterparts. Merely providing open access directly to any endpoint user is not conducive to and may interfere with efficient agency operations and the exercise of command and control functions. These considerations go well beyond the implementation of a uniform credentialing system for individual authentication and access. Conversely, the Bureau should be alert to §1426(b)(2)(A) being opportunistically enlisted to blunt competitive access and innovation under the banner of cybersecurity.

IV. Interoperability with Other Public Safety Communication Systems is Required

Public safety agencies currently utilize a large variety of proprietary communication systems, including LMR and PTT systems for voice, video management systems for video, and

various data sharing systems. The legacy of proprietary communications solutions particularly in the radio communications industry, which remain closed either through overt denial of access to interfaces or imposition of economic barriers through the imposition of high costs as in the case of P25 ISSI licensing and port usage costs, has led to the widespread communication interoperability problem faced by public safety today.

With the advent of the standardized MCx protocols and the buildout of FirstNet, there now exists a unique opportunity for FirstNet to act as a "universal mediator" and enable interoperability between any communication systems that implements the standard MCx protocols. This would then realize the originally envisioned nationwide network that enables interoperability between all first responders.

This is only possible, however, if an open philosophy of interconnection is adopted and facilitated with existing communication systems. Doing so also meets a broader implicit objective of achieving a resilient and adaptive national network communications environment that serves the safety and welfare of the public at large by providing first responders with the capabilities needed to connect by the best means necessary or available. How the FRNA chooses to exercise its authority and fulfill its duties will ultimately determine the ultimate adoption and use of FirstNet, and, beyond that, whether it serves to improve functional day to day interoperability or merely creates another silo which serves to only add to an already byzantine mosaic of disjointed communications environments.

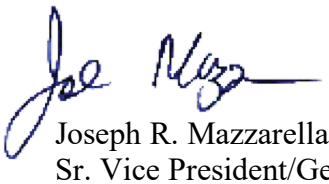
V. Public Safety Agencies Need to Choose the Tools That Work Best for Them

Public safety agencies are currently free to choose the wireless carrier that works best for their jurisdiction. Wireless coverage within that jurisdiction is certainly a primary consideration for choosing a carrier. First responders are routinely putting their lives on the line to serve and protect their communities. Encouraging or permitting any environment that serves to dissuade first responders from using the most effective communications tools in their arsenal or allowing commercial interests to block or impair free and open access between communications systems, particularly radio systems, would be contrary to the public interest and be a disservice to those serving it. In fact, 9/11 is testament to what happens when interoperability is nonexistent. Yet, in the 18 years since, the same protectionary market maneuvering continues unbated.

To the extent any LMR or LMR interconnected or related service provider is permitted to interconnect with a wireless carrier system and enjoy any form of priority or preemptive treatment, they must be required to be open and provide equal access for others to connect to the LMR and LMR interconnected or related service environments without any form of economic or other commercial discrimination. Similarly, among carriers the ability to interconnect in reasonable fashion should be required to ensure wireless public safety users in one network have ability to connect to the other. We believe that an interconnected eco-system of public and private public safety networks is critical to the nation's resiliency and ability to respond to the

increasing threats we face. To allow anything less is to turn a blind eye to some of the most painful lessons learned by our nation, and to do so would be to dishonor the many first responders and victims that have paid the price for this ongoing deficiency in 9/11 and countless numbers of reported cross agency communications failures since.

Respectfully submitted,



Joseph R. Mazzarella
Sr. Vice President/General Counsel

Mutualink, Inc.
1269 South Broad Street
Wallingford, CT 06492

Phone: (860) 559-7010
Email: jmazzarella@mutualink.net

September 26, 2019